

Amendments to the Specification

On page 1, after the title (line 1), please insert the following headings and paragraphs:

CROSS-REFERENCE TO RELATED APPLICATIONS

5 This application is the national phase filing, under 35 U.S.C. §371, of International Application No. PCT/DK2004/000692, filed October 8, 2004, the disclosure of which is incorporated herein by reference. This Application claims the benefit, under 35 U.S.C. §119(e), of US Provisional Application No. 60/509,669, filed October 8, 2003, the disclosure of which is incorporated herein by reference.

10

FEDERALLY-SPONSORED RESEARCH OR DEVELOPMENT

Not Applicable

BACKGROUND OF THE INVENTION

15

On page 6, line 19, please replace the heading with the following rewritten heading:

~~Invention:~~

SUMMARY OF THE INVENTION

20

Please replace the paragraph beginning on page 7, line 23 with the following rewritten paragraph:

25

This invention solves the problem of how to create and negotiate accountability paths for anonymous transactions dynamically adapted to context risk profile without creating linkability. An action of an individual is accountable without making multiple actions of individuals linkable. No single trusted party is able to link the identity of an individual to an action. Multiple different principles can be incorporated in the accountability path such as specific accountability incorporated through limited-show credentials, time locks, milestone verification, ~~serialised/parallelised~~ serialized/parallelized trusted party identity escrow etc. [[Manu]] Many of these can be built-into tamper-resistant and verifiable hardware eliminating the need to trust an organisation or human.

30

On page 11, after line 11, please insert the following heading:

DETAILED DESCRIPTION OF THE INVENTION

Please replace the paragraph beginning at page 11, line 13 with the following rewritten paragraph:

Fig. 3 shows the preferred setup for multi-application chip card infrastructure. The Chip Card (10) is communicating one-time only References to the Card Reader (42) using the communication channel (56) over ~~[[an]]~~ a fixednet IP-connection or any compatible open protocol such as a wireless channel. The Card Reader provides the connection to the Shop Computer (44) or in another embodiment done directly using for instance wireless communication protocols. The one-time only Reference is forwarded to the Service Provider (46) together with instructions encrypted inside the Chip Card. Client connect from his Client base (48) to take control of the transaction without revealing his real identity through a mixnet or other ~~anonymising~~ anonymizing network (50) or an Identity Provider/~~pseudonymising~~ pseudonymizing unit (54) through any communication channel (66). Depending on the encrypted instructions, the Service Provider (46) can verify anonymous payment or credential mechanisms directly (62) with financial institutions (52), or indirectly acting as a Trusted Party by forwarding chip card encrypted instructions to the Identity Provider (54).

Please replace the paragraph beginning at page 17, line 1 with the following rewritten paragraph:

This line of credit is on a periodically revolving basis transformed into Coins (tokens) using Digital Cash Technology, which is limited to show keys according to David Chaum (WO 0208865) or Stefan Brands (US5604805).

Please replace the paragraph beginning at page 26, line 24, with the following rewritten paragraph:

The Chip Card (10) receives standard payment information from the Shop Computer (44) through the Card Reader (20). Instead of encrypting and signing the message and then forwarding the message directly to the Financial Institution (52), the message is routed through a double layer of ~~pseudonymisers~~ pseudonymizers, making the Identity Provider (54) act as the Shop towards the Financial Institution (52) independently of the real Shop Id (44). The Chip Card (10) creates an encrypted message attached to a one-time only Reference which is then forwarded to the Service Provider, who decrypts the message. The message contains information as to the Relationship according to Fig. 4 and an additional encrypted message with at-

tached information to forward this message to the Identity Provider (54). The Identity Provider carries out the same operation to find an encrypted Chip Card payment message to forward to the Financial Institution naming the Identity provider the beneficiary of the payment.

- 5 Please replace the paragraph beginning at page 80, line 8 with the following rewritten paragraph:

Money ~~laundering~~ laundering

- It should be [[notes]] noted that in the preferred setup the electronic payment system in this invention has a built-in anti-money-~~laundering~~ laundering scheme in the closed loop monetary-system – money is transferred to/from bank accounts and only entering passing through
10 one transaction where taxes etc. can be ensured.

Please replace the paragraph beginning at page 80, line 14 with the following rewritten paragraph:

- 15 This scheme assumes that cost of transferring money to and from banking accounts is only covering the real cost – otherwise the anti-money-~~laundering~~ laundering scheme can be abused by banks to create an artificial fee structure with abnormal profits. In such case recirculation of electronic cash should be used to create a free cash flow until abnormal fees have been removed from the pricing structures.